

局域网可视化分析系统

1. 任务清单

	问题	具体内容
域计算机结构	数据准备	<ol style="list-style-type: none">1. 提取整理域控制器信息，来源：HASH 文件的文件名、Log 文件的文件名、Nbtscan 文件内容中的类型、Dsquery 文件的 desquery server2. 提取整理 DNS 服务器信息，来源：DNS 文件头部的 DNS server 键值对、Host-info 文件中网卡信息的 DNS3. 统计 servicePrincipalName 的种类，与已实现的不同节点对应的服务类型统计进行合并4. 统计操作系统类型，对应字段：operatingSystem5. 记录已采集过九种数据的节点，对应记录采集的文件类型6. IP 信息提取，来源：Log 数据、Nbtscan 数据、Port 数据、DNS 数据、Checkadmin 数据7. 组的统计，统计方法同 servicePrincipalName
	前端图形编码渲染	<ol style="list-style-type: none">1. 对不同服务器类型进行编码2. 对是否已采集过数据进行编码3. 对近期有登录的计算机进行编码4. 对不同组的计算机进行编码，编码方式同服务类型5. 对采集到 IP 数据的计算机的 IP 段进行编码
	交互	<ol style="list-style-type: none">1. 提供一个切换的接口，切换各种需要显示的编码2. 点击抽象的 bar 叶子节点，显示出对应的实际节点及相应的编码3. 节点展开时的编码类型切换4. 节点的自定义标识5. 给节点添加备注
域用户结构	数据准备	<ol style="list-style-type: none">1. 提取用户有效性信息，来源：csvde 中 userAccountControl 字段2. 提取组的信息，同计算机结构的组信息提取3. 提取在职时间，来源：whenCreated 字段

		4. 提取近期有登录用户信息，数据来源：lastlogonstamp
	前端图形编码渲染	1. 对在职时间进行编码 2. 对不同组的计算机进行编码，同计算机的编码 3. 对近期有登录的用户进行编码
	交互	1. 所有交互，同域计算机结构的交互
域组织单元	数据准备	1. 结构数据，来源：DN 字段
	前端图形编码渲染	1. 结构绘制
计算机与 IP 关系图	数据准备	1. 提取 Dsquery 文件中的 subnet 数据 2. 提取 Host-info 文件中的 TCP 信息
	前端图形编码渲染	1. 绘制计算机节点到 IP 段再到计算机的关系图，体现计算机的连通性 2. 绘制不同 IP 段的互通连线，体现 IP 的连通性
	交互	1. 计算机连线的 hover 高亮，提示 IP 信息 2. 计算机连通性与 IP 连通性的切换接口
计算机与用户关系图	数据准备	1. 提取 Checkadmin 文件中的权限数据 2. 查询登录关系时，log 中的名字对应数据库中的 sAMAccountName 字段，重新提取一遍数据
	前端图形编码渲染	1. 对用户对计算机的管理权限进行编码 2. 添加时间维度 3. 结构绘制
	交互	1. 可以进行自定义标注 2. 给节点添加备注文字 3. 选择不同的时间区间，选择然不同的节点连接情况
查询	数据准备	1. 提取 Host-info 文件中的软件或软件类别，来源：进程列表与安装软件
	图表渲染	1. 先展示查询结果在整体结构中所占的比例，通过点击某处的 bar，展开全部节点（多棵树组成的森林比较长，为清晰的知道查询结果在哪里，在结果处画一个气泡提示） 2. 互通性查询结果展示，高亮查询到的关系连线
	查询逻辑	1. 按照查询要求，写查询语句，连通前后端 2. 提供手动添加端口-服务、标识-服务

		<p>的接口, 用户添加后, 写入数据库, 可供后期的查询</p> <p>3. 异步获取下拉框选择框的内容</p>
相似用户分析	查询逻辑	1. 按照查询需求, 写查询语句, 连通后端数据与前端页面渲染
	交互	1. 切换到相似用户分析模式后, 提供各种查询条件, 供用户选择, 查询结果在用户结构图中实时渲染, 随着不断地搜索, 缩小目标范围, 找到相似用户
特殊用户分析	查询逻辑	1. 按照查询需求, 写查询语句, 连通后端数据与前端页面渲染
	交互	1. 切换到特殊用户分析模式后, 提供各种查询条件, 供用户选择, 查询结果在用户结构图中实时渲染, 随着不断地搜索, 缩小目标范围, 找到相似用户
特殊计算机或 IP 分析	查询逻辑	1. 按照查询需求, 写查询语句, 连通后端数据与前端页面渲染
	交互	1. 切换到特殊计算机或 IP 分析模式后, 提供各种查询条件, 供用户选择, 查询结果在用户结构图中实时渲染, 随着不断地搜索, 缩小目标范围, 找到相似用户
其它	数据准备	1. 页面头部的 4 项统计信息
	信息列表	<p>1. 可以导出查询结果, 一列或者几列</p> <p>2. 用户自定义列表字段后, 需要记住, 第二次的默认字段改为用户选择的</p>

2. 任务分工

开发人员	任务分工	任务编号	计划完成时间
梅鸿辉	域计算机结构	前端图形编码渲染 1-5	9.21
	域用户结构	前端图形编码渲染 1-3	9.24
	域组织单元	前端图形编码渲染 1	9.24
	计算机与 IP 关系图	前端图形编码渲染 1-2	9.25
	计算机与用户关系图	前端图形编码渲染 3	9.19
	相似用户分析	交互 1	10.11
	特殊计算机或 IP 分析	交互 1	10.14
魏雅婷	域计算机结构	交互 1-5	9.21
	域用户结构	交互 1	9.24
	域组织单元	数据准备 1	9.24
	计算机与 IP 关系图	交互 1-2	9.25
	计算机与用户关系图	数据准备 2	9.19

		前端图形渲染 1-2	9.27
		交互 1-3	9.30
	查询	图表渲染 1-2	10.11
	特殊用户分析	交互 1	10.14
顾宇辉	域计算机结构	数据准备 1、2、6	9.21
	计算机与 IP 关系图	数据准备 1-2	9.24
	计算机与用户关系图	数据准备 1	9.27
	查询	查询逻辑 1-3	9.30
	其他	数据准备 1	10.11
	特殊计算机或 IP 分析	查询逻辑 1	10.11
陈子熹	域计算机结构	数据准备 3、4、5、7	9.21
	域用户结构	数据准备 1-4	9.24
	查询	数据准备 1	9.27
	相似用户分析	查询逻辑 1	9.30
	特殊用户分析	查询逻辑 1	10.11
	其他	信息列表 1-2	10.14

3. 总体时间进度安排

日期	任务
9.18	分派任务，熟悉数据与程序
9.21	完成域计算机结构的绘制与交互
9.24	完成域用户结构与域组织单元的绘制与交互，计算机与 IP 关系图的数据准备工作
9.27	完成计算机与 IP 关系图绘制与交互，计算机与用户关系图的数据准备与
9.30	计算机与用户交互实现，相似用户分析查询逻辑
10.8	缓冲期，补前面阶段未完成计划
10.11	特殊用户分析查询逻辑，其他项的一项，查询结果的渲染，相似用户分析结果的渲染
10.14	特殊用户分析的结果渲染，特殊计算机或 IP 分析结果的渲染，信息列表功能完善